PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 :		(11) International Publication Number:	WO 93/05987
B60R 25/00, 25/04	A1	(43) International Publication Date:	1 April 1993 (01.04.93)

(21) International Application Number: PCT/GB92/01705

(22) International Filing Date: 17 September 1992 (17.09.92)

(30) Priority data:

9119924.0	17 September 1991 (17.09.91)	GB
9208554.7	21 April 1992 (21.04.92)	GB

(71) Applicant *(for AT BE CH DK GB GR IE IT LU NL SE only):* FORD MOTOR COMPANY LIMITED [GB/GB]; Eagle Way, Brentwood, Essex CM13 3BW (GB).

(71) Applicant *(for CA only):* FORD MOTOR COMPANY OF CANADA LTD. [CA/CA]; The Canadian Road, Oakville, Ontario L6J 5E4 (CA).

(71) Applicant *(for DE only):* FORD WERKE AG [DE/DE]; Werk Koln-Niehl, Henry Ford Strasse, Postfach 60 04 02, D-5000 Köln 60 (DE).

(71) Applicant *(for ES JP only):* FORD MOTOR COMPANY [US/US]; County of Wayne, Dearborn, MI 48120 (US).

(71) Applicant *(for FR MC only):* FORD FRANCE S.A. [FR/FR]; B.O. 307, F-92506 Rueil-Malmaison Cédex (FR).

(72) Inventor; and

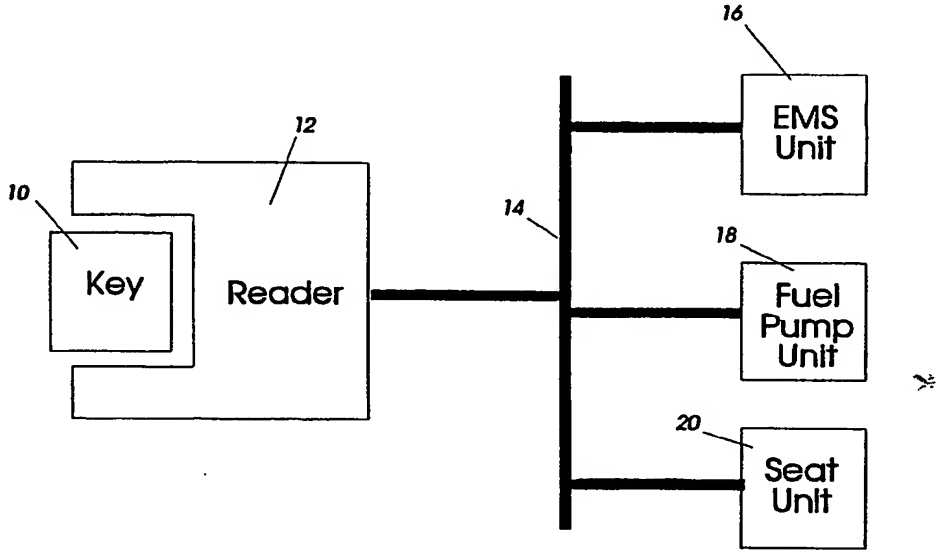
(75) Inventor/Applicant *(for US only) :* BIDDLECOMBE, David, Ernest [GB/GB]; Flat 6, 27 Shakespeare Road, Worthing, Sussex BN11 4AS (GB).

(74) Agent: MESSULAM, Alec, Moses; A. Messulam & Co., 24 Broadway, Leigh on Sea, Essex SS9 1BN (GB).

(81) Designated States: CA, JP, US, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, SE).

Published
With international search report.

(54) Title: VEHICLE SECURITY SYSTEM



(57) Abstract

A vehicle security system, comprises a coded key (10), a reader (12) for reading the code of the key (10) and generating an encoded electrical signal, a data transfer bus (14) connected to the reader, and a plurality of units (16, 18, 20) connected to the data transfer bus (14) and rendered operative only upon receipt of a predetermined valid code from the reader. Each unit (16, 18, 20) is arranged upon receiving an invalid code to transmit an error code over the data transfer bus (14) to the reader (12) or to other units connected to the bus, and upon detection of an error code on the bus from at least selected ones of the units (16, 18, 20), other units (16, 18, 20) connected to the bus are rendered inoperative even if the latter units had received valid codes.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	FI	Finland	MN	Mongolia
AU	Australia	FR	France	MR	Mauritania
BB	Barbados	GA	Gabon	MW	Malawi
BE	Belgium	GB	United Kingdom	NL	Netherlands
BF	Burkina Faso	GN	Guinea	NO	Norway
BG	Bulgaria	GR	Greece	NZ	New Zealand
BJ	Benin	HU	Hungary	PL	Poland
BR	Brazil	IE	Ireland	PT	Portugal
CA	Canada	IT	Italy	RO	Romania
CF	Central African Republic	JP	Japan	RU	Russian Federation
CG	Congo	KP	Democratic People's Republic of Korea	SD	Sudan
CH	Switzerland			SE	Sweden
CI	Côte d'Ivoire	KR	Republic of Korea	SK	Slovak Republic
CM	Cameroon	LI	Liechtenstein	SN	Senegal
CS	Czechoslovakia	LK	Sri Lanka	SU	Soviet Union
CZ	Czech Republic	LU	Luxembourg	TD	Chad
DE	Germany	MC	Monaco	TG	Togo
DK	Denmark	MG	Madagascar	UA	Ukraine
ES	Spain	ML	Mali	US	United States of America

Title

Vehicle Security System

Field of the invention

The present invention relates to a security system for a vehicle and may be applied to motor vehicles, boats and aircraft to prevent theft and unauthorised use.

Background of the invention

Vehicle thefts have reached the stage of causing serious public concern and much research has been devoted to enhancing vehicle security. Conventionally, purely mechanical devices, i.e. locks, have been used to prevent access to the interior of the vehicles or inhibit operation of the steering or the gearbox. There have also been available in the so-called after market simple electrical immobilisation devices which detect tampering and inhibit engine operation by open circuiting units such as the starter motor or fuel pump, or short circuiting units such as the crankshaft position sensor or the low tension lead of the ignition coil.

More recently, vehicle manufacturers have considered incorporating more sophisticated systems as original equipment and the present invention is a development of one such system which is similar, for example, to that described in US Patent No. 4,366,466. Such systems include a passive encoded circuit or key which can be read by a reader in the vehicle. The code read from the key is compared with a stored code and the vehicle is immobilised in the event of a mismatch.

A serious problem to the immobilisation of a vehicle is presented by the possibility of the security system being bypassed by what is termed "hot wiring". For example, if

immobilisation is effected by cutting off the power supply to the starter motor or the fuel pump, then directly connecting these units to the vehicle battery live terminal would render the security system useless.

To avoid this problem, the reader does not simply operate relays connected to such units, but communicates with them in code over a data transfer bus. As each unit connected to the bus can only be activated by receiving the correct code from the reader, bypassing the security simple is not possible. The would be thief must emulate the encoded signals generated by the key reader and this is not easily achievable.

A difficulty with even this system is that, for servicing purposes, it must be possible to replace a unit in the event of failure. For this reason, new units cannot be encoded prior to being fitted to a vehicle. Should a thief obtain, for example, a new engine management system computer and plug it in the place of an existing one, the security will be inoperative as the new computer will automatically learn the existing code of the vehicle key.

Object of the invention

The present invention therefore seeks to provide an improved security system in which replacement of individual units will not allow the vehicle to function correctly.

Summary of the invention

According to the present invention, there is provided a vehicle security system, comprising a coded key, a reader for reading the code of the key and generating an encoded electrical signal, a data transfer bus connected to the reader, and a plurality of units connected to the data transfer bus and rendered operative only upon receipt of a predetermined valid code from the reader, wherein each unit

is arranged upon receiving an invalid code to transmit an error code over the data transfer bus to the reader or to other units connected to the bus, and upon detection of an error code on the bus from at least selected ones of the units, other units connected to the bus are rendered inoperative even if the latter units had received valid codes.

The units referred to above can be essential or ancillary units. Examples of essential units are the engine management computer, the fuel pump, starter motor, braking system, or the transmission system. Ancillary units may include modules for operating the electric windows, seats, instrument cluster, lights and so on. The nature of the response to an error code by the system can be dependent on the unit which generates the error code.

For example, if it is found that a safety critical system is not responding correctly, then total immobilisation may be selected. However, if a radio or window unit responds with an error code, then it may suffice for the system to alert the driver of the failure.

The verification of system integrity which results from the transmission of error codes along the bus offers a first advantage of improving vehicle safety. A vehicle will for example not be allowed to start if the transmission or brakes have failed. The starter motor can be prevented from draining the battery if the engine has been disabled by the engine management computer.

The system however also offers improved security against theft. Supposing for example that a new key and reader unit is fitted and the engine management computer is replaced. On switching on, the reader will send a code to the new engine management computer which will record it and enable the engine to operate with the new code. However, the error code generated by another essential unit, such as the fuel

pump or the starter motor, will alert the system to the attempted theft and will again disable the engine management system. By virtue of the fact that codes are distributed around the vehicle, many in units which are inaccessibly located, roadside theft is effective prevented and as full system shut down can result, the thief is given little indication as to the source of the error code.

Of course, a person having the correct key and reader will have no difficulty replacing a unit. Each unit will in this case be correctly matched when the new one is added to the system for the first time and as no error code will be generated, the null code with which the new unit is shipped will be replaced by the correct system code.

To prevent theft by simultaneous multiple replacement of units, the detection of more that one null code may be used to cause system shut down unless all units are new. This does not interfere with authorised repair as units can be replaced one at a time but does inhibits theft. The ability to operate with only new and uncoded units throughout the vehicle must of course be retained to allow the vehicle to be manufactured without having to manufacture matched units and readers.

To allow the vehicle to be driven and tested in a factory during manufacture, it may be possible to enable all units in the vehicle using a special key generating a null code without causing all the units to be reconfigured. Once the vehicle units have been configured with a key not containing the null code, the null code will cease to function.

It is convenient for the electronic key of the invention to be integrated with a conventional mechanical key for operating the door locks and the ignition lock. For example, the circuit can be embedded within the shaft or the handle of the key. As a further possibility, the electronic key may be formed within the key fob.

The key circuitry can be a passive circuit (no internal power supply) energised by a magnetic field or electro-magnetic radiation emitted by the reader. Alternatively, power can be coupled to the key circuit by contacts. The encoded signal may in turn be transmitted to the reader by radio, infra red or electrical contact methods. It is preferred to use contactless coupling as the operation of the electronic security system will then be totally transparent to the user and will operate reliably each time the ignition key is inserted into the lock.

As the system of the invention already has the facility to disable units even when they have received their valid codes, this facility may be utilised to disable operation of the vehicle under other conditions. For example, the key may be encoded with time or mileage information to prevent the system from operating when a time or mileage limit has been exceeded. Such a facility may be brought into operation, for example, with hire car fleets to prevent theft after the legal hire period has expired.

Brief description of the drawings

The invention will now be described further, by way of example, with reference to the accompanying drawings, in which :

Figure 1 is a schematic diagram of a security system of the invention, and

Figure 2 shows a flow chart for the operation of the system illustrated in Figure 1.

Description of the preferred embodiment

In Figure 1 an electronic key 10 is constructed in the form of a passive transponder built into the handle of an otherwise convention ignition key of a motor vehicle. When

the ignition key is inserted in the ignition lock, the electronic key is located within range of a stationary reader 12 which while the ignition lock is being turned interrogates the transponder 12. The electronic key 10 and reader 12 will not be described herein in detail as they are known per se, a suitable example being described in detail in US Patent No. 5,053,774.

For the present purposes, it suffices to know that after the key 10 is inserted in the reader 12, the latter transmits electromagnetic radiation which powers the transponder circuit of the key 10. The latter emits an encoded radio signal which is received and decoded by the reader 12. The received code is compared with a predetermined code in the reader 12. In the event of a match, a digital encoded signal is transmitted over a data transfer bus 14 to various units 16, 18 and 20 distributed about the vehicle.

It has previously been proposed to replace the dedicated wiring loom of a vehicle by a bus which includes power lines and data transfer lines carrying serial data. The bus 14 in the present invention may be such a bus. All the electrical components of the vehicle are connected to the same bus by units or modules which are programmed to recognise their own address and which act to detect and implement instructions on the data bus intended for their associated components. For example, if the control unit associated with the headlights has address No. 38, then it will detect on signals on the common bus 14 with that address. If the driver wishes the headlights to be turned on, then on receiving the instruction from a central control circuit, the unit will effect a connection between the headlights and the common power lines through an electronic switch or a relay built into the unit. The advantage of such a wiring loom system is that it requires fewer wires, is easier to install and avoids the need for a manufactures to produce a wide variety of looms. The same wiring can be used for all vehicles and only the programming of the system will vary

between vehicle models having different equipment specifications.

The preferred embodiment of the present invention makes use of the presence of a data bus in the vehicle to provide increased security against theft by storing security codes in several of these units or modules.

There will be some modules the operation of which is essential to the safe functioning of the vehicle. Two such essential units are shown by way of example in Figure 1, first unit 16 being integrated into the engine management system (EMS) which controls spark timing and fuelling of the engine and the second being a unit 18 which turns on the fuel pump. Further examples of essential units would be any connected to the starter motor, to a traction control system, to an active suspension system or to an anti-lock breaking system.

Other modules will operate ancillary equipment, such as the seat unit 20 shown in Figure 1 which allows adjustment of the seat position. There are many further examples of ancillary equipment, such as the radio, instrument dials, there being too many to provide an exhaustive list.

In the illustrated embodiment, codes matching the output code of the reader 12 on receiving the correct key 10 are stored in several, if not all of the control units distributed around the vehicle. If they receive the wrong code from the reader, for example if a thief succeeds in by-passing the reader 12 or if the reader is replaced by a reader stolen from another vehicle, then none of the encoded units will operate.

A problem arises on account of the fact that replacement units are provided uncoded and record the first code they receive when installed in a vehicle in a one time programmable (OTP) memory. This means that armed only with

a few essential units and a reader, a thief could circumvent the security system.

This possibility is reduced in the present invention in that the units 16, 18, 20 do not simply receive control signals from the bus 14 but transmit back information on their status if they fail to recognise the code that they receive. This information can be read either by the reader 12 or by any of the other units 16, 18, 20 which may then be programmed to take the appropriate action having regard to the identity of the failed unit.

The strategy adopted in the preferred embodiment of the invention takes into account whether the unit is an essential or an ancillary unit when deciding on the action of the taken. If a unit regarded as essential fails, then the vehicle is immobilised. This prevents theft and is also a safeguard against the vehicle being driven away in a dangerous condition if the essential component has failed for some other reason. If another unit fails, then less severe action can be taken such as warning the driver of the fault. However, even with ancillary units, the simultaneous failure of several units to recognise the code transmitted by the reader could signify attempted theft and be used to immobilise the vehicle completely.

The advantage of distributing codes in many places around the vehicle are numerous. First, the units are usually in inaccessible locations, such as behind the instrument panel, inside the door trim or within the housing of the fuel pump. As a consequence, even with a complete new set of units and a new key and reader unit, several hours would be required in changing the units before the vehicle could be driven away. This makes theft from the roadside extremely difficult. Crime statistics suggest that any system requiring more than fifteen to twenty minutes to by-pass will prevent theft in the majority of cases.

Stealing a vehicle to break it up for spare parts will no longer be viable as the expensive units will not function in any other vehicle once they have been programmed for a particular code. Also because numerous new units would need to be installed before the vehicle could be put back into a state in which it could be re-sold, even the professional thief would be deterred.

The units 16 to 18 and the reader include programmed processors and their operation in the preferred embodiment of the invention is best understood by reference to the flow chart of Figure 2.

When the key 10 is inserted in the reader 12, the processor in the latter compares the read key code with a code previously stored into the OTP memory of the reader. If there is a mismatch, then it is determined if the reader contained the null code (for example Hex FFFFF), i.e. if the reader had been previously encoded. If not, then the received code is stored in the OTP of the reader and thereafter the reader will only respond to that same key code. In the event of a mismatch between the key code and a previously encoded reader, then no output data is placed on the bus 14 and all units, essential and ancillary, will remain disabled.

If there is a correct match between the key and the reader, then it is determined if the reader contained a null code. If so a null code is placed on the data bus otherwise a security code associated with the key code is placed on the bus.

On detecting a code on the bus, each unit compares the code with that in its own OTP memory. In there is a match, then the unit is enables and its associated electrical component or system is rendered operational. In the event of a mismatch, however, it is ascertained if the OTP memory of the unit contained the null code. If not, that is to say

if the unit had previously been programmed and its internal code did not match the received code, then not only is the unit disabled but an error code in placed on the data bus to warn other units connected to the bus of the defect.

If the unit did contain a null code, that is to say it was not previously programmed, then it is enabled and a warning code is placed on the bus to warn of the presence of a new and as yet unconfigured unit.

The reader is programmed to analyse any error or warning signal placed on the bus by the other unit. If an essential unit reports a mismatch, then it is preferred to send signals to disable all units, even those which received their valid codes. If several units reply with error codes, then it is again desirable to disable all units. When only one ancillary unit fails to recognise the security code, then it may suffice to warn the driver.

If the reader receives several warning signals, indicating an attempt to replace several units at the same time, then it will again disable all units rapidly. Even though the new units will have been enabled for a short time, their OTP memory will not have been reprogrammed and repeated attempts will all lead to failure to start the vehicle. If however there is only one such warning signal, then this is taken to be a repair by an authorised dealer and after a time delay, if the unit has not been disabled, it will write the security code into its OTP memory.

It will be noticed that if a null key is used in a new reader and the signals are sent to new units, the entire system will operate correctly with null codes and without any writing of data to the various OTP memories. This facility enables all cars to remain uncoded while being manufactured and tested. The first time an encoded key is used, however, its coded will be written to the reader and into all the units. For this purpose, the facility of

disabling all units when several null codes are detected can itself be disabled either by the fact that the reader itself contained a null code or by the fact that all units without exception have responded with a null code warning.

It is possible for the code read by the reader 12 from the key 10 to contain data in addition to the security code. For example, the key may contain data personal to the driver which is written to a E-PROM in the key by the reader 12. Such data may include seat positions, preferred radio frequencies and so on. It is also possible to stored personal fuelling and spark timing maps which alter the performance of the vehicle in dependence upon the driver. For example, performance may be limited for an inexperienced driver.

The presence of programmable memory in the key 10 allows further security features to be incorporated into the system. For example, a car hire company may record time and mileage information to limit the hire period and immobilise the vehicle outside the period of permitted use. This would prevent a thief from hiring a car legally, copying the key, then returning to steal it.

It should be stressed that the description given above is only by way of non-limiting example and that various modification may be made without departing from the scope of the invention as set out in the appended claims. The key and its reader need not be integrated into the ignition key and lock and one may use other forms of key capable of generating an electrical code.

The reader may, if desired, be integrated into one of the units 16 to 20, preferably the EMS unit 16. Such a construction can be manufactured with less expense and reduces the risk of tampering with the output signal of the reader.

As a further possibility, the described OTP memories may be replaced by EEPROM's which can be reprogrammed, the writing to the EEPROM being restricted to once by the program stored within the unit when it is manufactured. Such construction offers the possibility of enabling the manufacturer to reprogram the units if they are returned for reconditioning, but it is less desirable from the security point of view.

The data bus 14 described above is a serial bus and the reader 12 acts as the central unit from which other units are controlled. Such system architecture is also not fundamental to the invention and one may use a parallel with the units arranged in a ring or a star network. Furthermore, each unit may determine its own state depending on the signals on the data bus, instead of relying on signals from a central controller.

CLAIMS

1. A vehicle security system, comprising a coded key (10), a reader (12) for reading the code of the key (10) and generating an encoded electrical signal, a data transfer bus (14) connected to the reader, and a plurality of units (16,18,20) connected to the data transfer bus (14) and rendered operative only upon receipt of a predetermined valid code from the reader, characterised in that each unit (16,18,20) is arranged upon receiving an invalid code to transmit an error code over the data transfer bus (14) to the reader (12) or to other units connected to the bus, and upon detection of an error code on the bus from at least selected ones of the units (16,18,20), other units (16,18,20) connected to the bus are rendered inoperative even if the latter units had received valid codes.

2. A system as claimed in claim 1, wherein the units include units essential to safe operation of the vehicle and units associated with ancillary vehicle equipment, the nature of the response to an error code by the system being dependent on the function of the unit which generates the error code.

3. A system as claimed in claim 2, in which all units are rendered inoperative in response to an error code from an essential unit.

4. A system as claimed in claim 2 or 3, in all units are rendered inoperative in response to an error code from two or more ancillary units.

5. A system as claimed in any preceding claim, wherein each unit when first installed in a vehicle contains a null code and wherein the first non-null security code sent by the data bus (14) to the unit is stored in the memory of the unit.

6. A system as claimed in claim 5, wherein a unit containing a null code is operative to transmit a warning code to the reader or to other units connected to the bus prior to writing the security code to its memory.

7. A system as claimed in any preceding claim, wherein the key (10) is integrated with a conventional mechanical key for operating the door locks and the ignition lock.

8. A system as claimed in any preceding claim, wherein the key (10) comprises a passive circuit energised by a magnetic field or electro-magnetic radiation emitted by the reader (12).

9. A system as claimed in any preceding claim, wherein the key code comprises data in addition to the security code required to enable the encoded units (16,18,20).

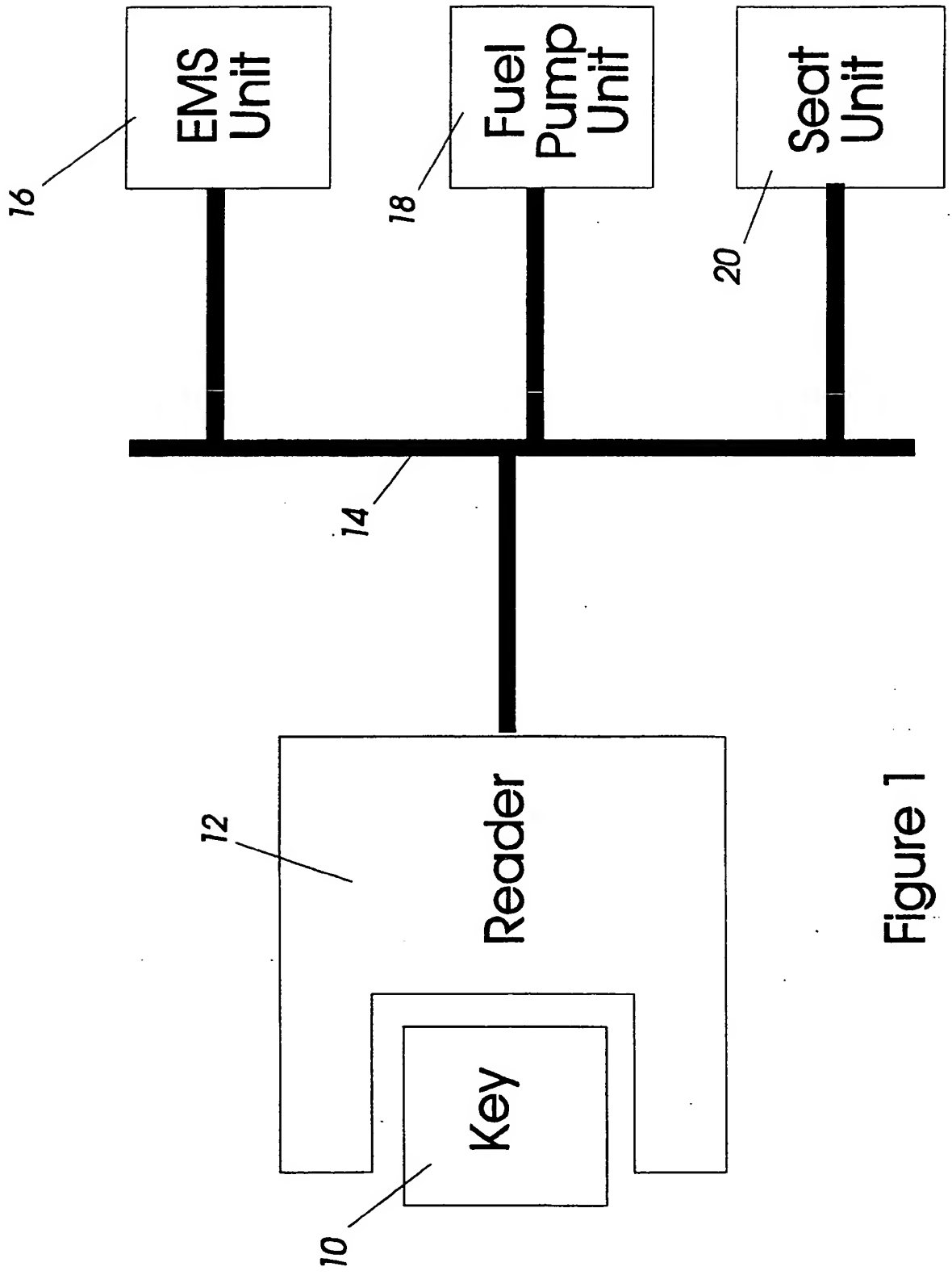


Figure 1

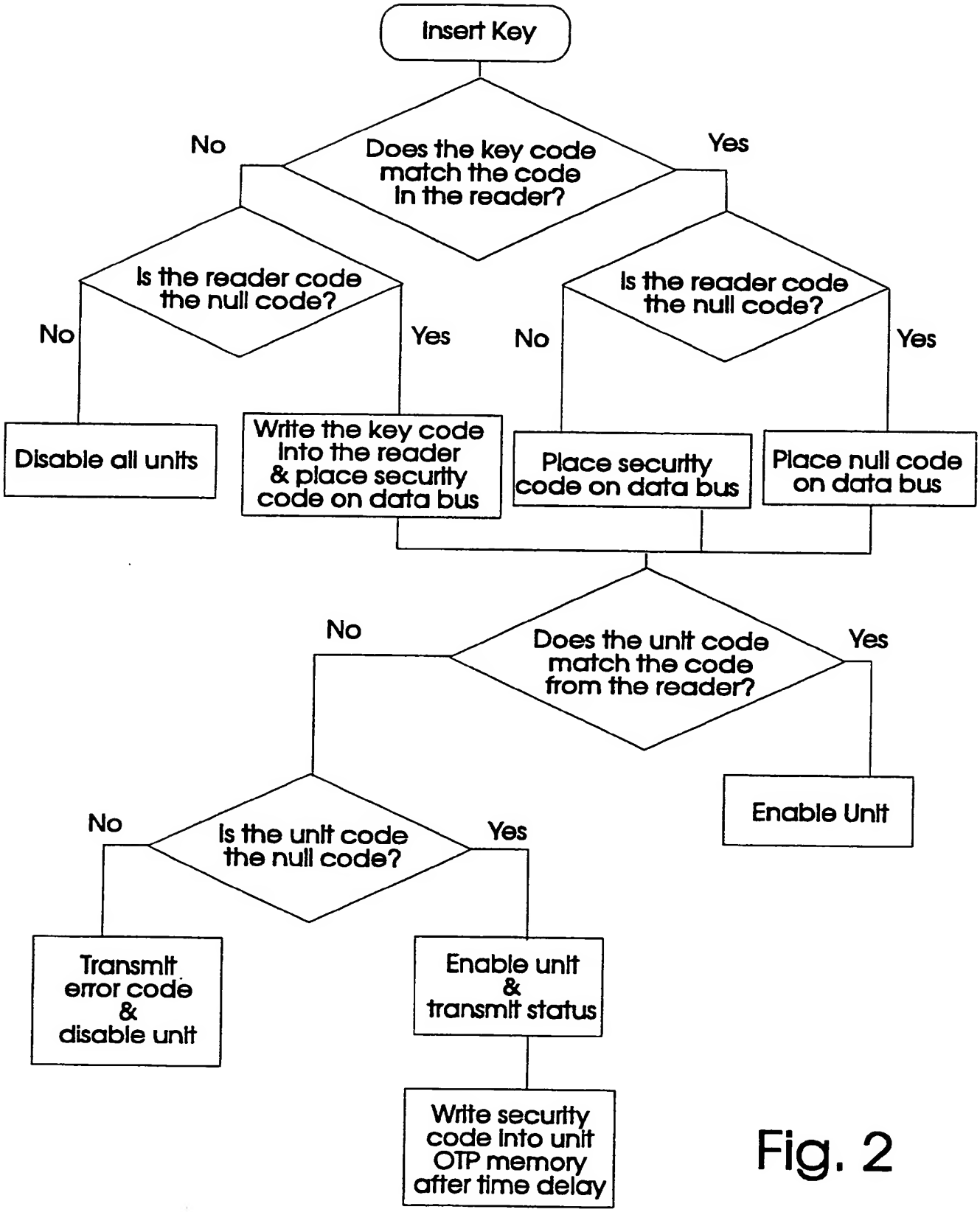


Fig. 2

INTERNATIONAL SEARCH REPORT

International Application No PCT/GB 92/01705

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all)[6]

According to International Patent Classification (IPC) or to both National Classification and IPC

Int.Cl. 5 B60R25/00; B60R25/04

II. FIELDS SEARCHED

Minimum Documentation Searched[7]

Classification System	Classification Symbols
Int.Cl. 5	B60R

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched[8]

III. DOCUMENTS CONSIDERED TO BE RELEVANT[9]

Category °	Citation of Document,[11] with indication, where appropriate, of the relevant passages[12]	Relevant to Claim No.[13]
P,X	GB,A,2 251 503 (INTELEPLEX CORPORATION) 8 July 1992 see page 4, line 10 - page 5, line 9 see page 7, line 13 - line 24 see page 14, line 12 - line 17; figures ---	1,7
A	EP,A,0 372 741 (ROVER GROUP LIMITED) 13 June 1990 see column 2, line 26 - column 3, line 16 see column 4, line 24 - line 38 see column 5, line 36 - column 6, line 21 see figure ---	1,7
A	US,A,4 477 874 (IKUTA ET AL.) 16 October 1984 see column 2, line 11 - line 27; figures 1,2 --- -/--	1,8

° Special categories of cited documents :[10]

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
16 DECEMBER 1992	15. 01. 93
International Searching Authority	**Signature of Authorized Officer**
EUROPEAN PATENT OFFICE	AREAL CALAMA A.

Form PCT/ISA/210 (second sheet) (January 1985)

III. DOCUMENTS CONSIDERED TO BE RELEVANT (CONTINUED FROM THE SECOND SHEET)

Category °	Citation of Document, with indication, where appropriate, of the relevant passages	Relevant to Claim No.
A	EP,A,0 105 774 (JEAN-PIERRE VERINE) 18 April 1984 see claims; figures	1

ANNEX TO THE INTERNATIONAL SEARCH REPORT ON INTERNATIONAL PATENT APPLICATION NO. GB 9201705 SA 65104

This annex lists the patent family members relating to the patent documents cited in the above-mentioned international search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information. 16/12/92

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB-A-2251503	08-07-92	DE-A- 4123666	09-07-92
EP-A-0372741	13-06-90	GB-A- 2227791	08-08-90
		JP-A- 2279429	15-11-90
US-A-4477874	16-10-84	JP-C- 1495571	16-05-89
		JP-A- 57090236	04-06-82
		JP-B- 63045332	08-09-88
EP-A-0105774	18-04-84	FR-A- 2533516	30-03-84
		JP-A- 59081239	10-05-84

EPO FORM P0479

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82